

FILED
DISTRICT COURT OF GUAM

SEP 25 2020

UNITED STATES DISTRICT COURT

for the
District of GuamJEANNE G. QUINATA
CLERK OF COURT

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information associated with mobile phone number (671) 967-4452 that is stored
at premises owned, maintained, controlled, or operated by PTI Pacifica Inc. dba
IT&E, 122 Harmon Industrial Park Rd, Tamuning, Guam 96913
(Further described in Attachment A)

Case No. MJ-

20-00104

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Information associated with mobile phone number (671) 967-4452 that is stored at premises owned, maintained, controlled, or operated by PTI Pacifica Inc. dba IT&E, 122 Harmon Industrial Park Rd, Tamuning, Guam 96913. Further described in Attachment A.

located in the _____ District of _____ Guam _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B which incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 USC 841(a)(1), 843(b), 846, & 856	Distribution of Methamphetamine, Use of Communication Facility, Conspiracy, and Maintaining Drug-Involved Premises

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of _____ days *(give exact ending date if more than 30 days)* _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SHAWN AYUYU, Task Force Officer, DEA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*

Date:

9/25/20

City and state: Hagatna, Guam

Judge's signature

MICHAEL J. BORDALLO, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Shawn A. Ayuyu, being duly sworn, hereby depose and state as follows:

A. Background of Affiant

1. I am a Police Officer III with the Guam Police Department and have been so employed since October 2007. I have been assigned to the Neighborhood Patrol Division, Property Crimes Unit, Special Operations Division (SOD), Special Weapons and Tactics (SWAT), Marine Patrol Division, Special Investigations Section (SIS) and the Mandana Drug Task Force (MDTF). I completed the Secret Service's National Computer Forensics Institute (NCFI) training in July, 2018, which certified me to perform digital forensic analysis on a variety of media devices such as computer hard drives, mobile devices such as androids and cell phones using a Forensic Evidence Recovery Device (FRED).

2. I am also a Task Force Officer with the U.S. Drug Enforcement Administration (DEA) and have been so since August of 2018. As a Task Force Officer, my job assignment includes, but is not limited to, the investigation of violations of Title 21, United States Code, Sections 841(a)(1), 846, 843(b) and 856, which includes the detection, identification, and apprehension of those individuals involved in narcotics trafficking offenses.

3. As a Task Force Officer, I have participated in investigations of criminal violations of the Federal Controlled Substances Act. I have also participated in undercover investigations involving the purchase of controlled substances, assisted in the execution of state, local and federal search warrants relating to controlled substances and have conducted numerous surveillance and controlled deliveries in connection with narcotic investigations.

4. I am familiar with the operation of illegal drug trafficking organizations (DTOs) in the United States and DTOs with a foreign nexus. I know from my training, experience and

discussions with other law enforcement officers that importers and distributors of controlled substances often use cellular phones to communicate instructions, plans, and intentions to their criminal associates and to report on the progress of their criminal activities. I am aware that evidence of these instructions, plans, intention, reports and general discussions of criminal activity are sent or received in the form of SMS text messages, incoming and outgoing call histories or voice messages left in personal voice mail systems. I am familiar with the methods in which text messages are sent and received and know that third party phone applications, most commonly referred to as “Apps,” are widely used.

5. The information contained within this affidavit is based upon my personal observations, training, and on information related to me by other law enforcement officers and investigators as set forth more fully herein. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Because the purpose of this affidavit is to set forth probable cause, your affiant has not included each and every fact known to the affiant in connection with this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of 21 U.S.C. §§ 841(a)(1), 843(b), 846 and 856 are located within the electronic device, said information is stored at premises owned, maintained, controlled or operated by **PTI Pacifica Inc. dba IT&E Telecommunication**, as identified in Attachment A.

B. Purpose of Affidavit

6. This affidavit is made in support of the issuance of a search warrant to obtain judicial authority for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by **IT&E**, a Telecommunication provider

headquartered at 122 West Harmon Industrial Park Rd, Tamuning 96913, Guam. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require IT&E to disclose to the government, records and other information in its possession pertaining to the subscriber or customer associated with the account, including the contents of communications.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 856, 841(a)(1), 843(b), and 846 (conspiracy to distribute methamphetamine hydrochloride), have been committed by Aaron Matthew PANGELINAN utilizing phone number 671-967-4452 and I believe there is probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

C. Jurisdiction

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i) and “is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(ii).

D. Facts Establishing Probable Cause

9. In November 2019, investigators with the Guam Resident Office received information regarding the drug trafficking activities of Aaron Matthew PANGELINAN (hereafter referred to as PANGELINAN). The Source of Information (SOI) stated that

PANGELINAN is distributing gram quantities of methamphetamine on Guam and that the SOI is able to purchase methamphetamine from PANGELINAN. Investigators conducted an open source check and found that PANGELINAN had previously resided in Washington State, a known source state of methamphetamine for Guam. A check with Department of Motor Vehicle records revealed that PANGELINAN listed 135 Naki Street in Ordot, Guam, as his residence. A search of the National Crime Information Center revealed that PANGELINAN has a prior arrest for Possession of a Controlled Substance, Family Violence, and Violation of a Court Order Protection Order, while he resided in Washington State.

10. Between December 2019, and January 2020, investigators with the Guam Resident Office (GRO) conducted controlled buys with PANGELINAN utilizing a Drug Enforcement Administration Confidential Source (CS). The CS successfully purchased at total of 22.6 gross grams of suspected methamphetamine from PANGELINAN. Prior to conducting the controlled buys, investigators also conducted controlled calls to PANGELINAN at 671- 967-4452 which was provided to investigators by the CS.

11. Sometime in early December 2019, investigators conducted a controlled purchase of methamphetamine from PANGELINAN. Investigators directed the CS to call PANGELINAN at 671-967-4452 to arrange the purchase of methamphetamine. PANGELINAN did not answer the CS' initial call. The CS was then instructed to text PANGELINAN indicating that the CS wanted to purchase methamphetamine. PANGELINAN responded to the CS' text message saying "Stand by". PANGELINAN and the CS continued to text each other until PANGELINAN called the CS and instructed the CS to proceed to PANGELINAN'S residence. Prior to meeting with PANGELINAN, the CS was outfitted with an audio/video monitoring device which enables investigators to monitor the controlled purchase. The CS went to

PANGELINAN'S residence at 135 Naki Street Chalan Pago and met with PANGELINAN. The CS successfully purchased approximately 7.9 gross grams of methamphetamine and soon thereafter met with investigators who seized the suspected methamphetamine. A field test was conducted on the suspected methamphetamine which yielded a presumptive positive result for the presence of methamphetamine.

12. On a subsequent controlled purchase also in December 2019, the CS again contacted PANGELINAN via cell phone at 671-967-4452 and PANGELINAN agreed to sell the CS methamphetamine. Prior to the controlled buy, the CS was again outfitted with an audio/video monitoring device. On the same date, the CS met with PANGELINAN at PANGELINAN'S residence. Upon arriving at the residence, the CS was informed by PANGELINAN that he was waiting for the methamphetamine to be dropped off. During the controlled purchase, investigators overheard PANGELINAN receive a phone call from an unknown individual. After PANGELINAN ended the call, PANGELINAN informed the CS that the "meth" is on its way. Investigators noted the time PANGELINAN received the phone call. A short time later, an unknown male individual operating a dark colored SUV like vehicle arrive at PANGELINAN'S residence. The CS stated that the unknown male individual proceeded to a back room that was adjacent to where the CS was waiting. The unknown male and PANGELINAN met in the room. PANGELINAN later emerged from the room and handed the CS the methamphetamine. The CS subsequently departed PANGELINAN'S residence and met with investigators who seized approximately 2.5 grams of the suspected methamphetamine. A field test was conducted on the suspected methamphetamine which yielded a presumptive positive result for the presence of methamphetamine.

13. On January 22, 2020, investigators subsequently obtained PANGELINAN'S phone toll records from service provider IT&E which was registered as a pre-paid account. The information contained in the records was consistent with investigators' noted time frame of the call and the audio recordings of the controlled purchase.

14. On a subsequent controlled purchase, which occurred in September 2020, investigators again utilized a CS to purchase methamphetamine from PANGELINAN. The CS was instructed to place a controlled phone call to PANGELINAN at 671-967-4452 to arrange the purchase of methamphetamine. The CS placed the call and PANGELINAN agreed to sell the CS methamphetamine. Subsequently, the CS, who was outfitted with an audio/video monitoring device, met with PANGELINAN at PANGELINAN'S residence. The CS can be heard talking to PANGELINAN over the monitoring device. During the controlled purchase, the CS observed PANGELINAN walk into the garage area and then walked back out to the vehicle to complete the purchase of methamphetamine. Investigators met with the CS and seized the methamphetamine and a field test was conducted. The test yielded a presumptive positive result for the presence of methamphetamine.

15. On September 22, 2020, investigators were able to obtain the registered account holder of phone number 671-967-4452 from service provider IT&E. According to IT&E records, 671-967-4452 is a pre-paid account. The account is still in service.

D. Relevant Facts on Wireless Services and Technology

16. In my training and experience, I have learned that PTI Pacifica Inc. dba IT&E is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and un-retrieved voicemail, text, and multimedia messages for IT&E subscribers may be located on the computers of IT&E. Further, I am aware

that computers located at **IT&E** contain information and other stored electronic communications belonging to unrelated third parties.

17. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of **IT&E** for weeks or months.

18. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging" or "wireless messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by **IT&E** for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

19. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may

also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

20. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

21. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

22. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the

length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

23. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the

foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

E. Information to Be Searched and Things to Be Seized

25. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require **IT&E** to disclose to the government copies of the records and other information (including the content of communications) described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

F. Request for Nondisclosure Order

26. Your affiant requests, pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(a)(A), that IT&E for a period of 90 days, be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for a period of ninety days from the date the warrant is issued. The government submits that such an order is justified because notification of the existence of this warrant could jeopardize the ongoing investigation, disclosure would give the subscribers an opportunity to notify confederates of this warrant and/or to destroy, conceal or otherwise obfuscate evidence.

G. Request for Sealing

27. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

H. Conclusion

28. Based on my training and expertise, I know that drug traffickers frequently use cellular telephones to communicate and discuss illegal activity. I also know that cellular telephones, specifically the cellular providers described in Attachment A, retain information as to the most recent numbers dialed, duration of calls, and caller identification information from recent incoming calls, voice mail and text messaging. Additionally, I know that cellular providers keep digital information stored in servers. This information is necessary to identify associates and other co-conspirators.

29. Based on my training and experience, I know that in addition to voice communication, people using cellular telephones to facilitate criminal activity can communicate with each other by sending text messages and/or e-mail messages, which can and frequently are stored in the electronic data of the cellular telephone handset and servers. I believe a review of the text messages, call logs and/or e-mail messages stored in, specifically the server described in Attachment A will provide investigative leads and evidence relevant to this ongoing criminal investigation.

30. Based on my training and experience and the information contained in this Affidavit, investigators believe that Aaron Matthew PANGELINAN is currently involved in the trafficking and distribution of methamphetamine, a violation of Title 21, United States Code, Sections 841(a)(1), 843(b), 846 and 856, and that evidence of that criminal activity can be found in the text messages and stored electronic data accessible from specifically the cellular service provider described in Attachment A.

31. Based on the foregoing, I respectfully request that a search warrant be issued authorizing the search of specifically the cellular service provider for calls logs, SMS text messages described in Attachment A and seize the items as set forth and in Attachment B, all of which constitutes evidence, fruits or instrumentalities of the aforementioned crime(s).

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

//

//

//

//

33. The government will execute this warrant by serving the warrant on **IT&E**. Because the warrant will be served on **IT&E**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

FURTHER AFFIANT SAYETH NAUGHT.

SHAWN A. AYUYU
Task Force Officer
Drug Enforcement Administration

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with mobile phone number (671) 967-4452 that is stored at premises owned, maintained, controlled, or operated by **PTI Pacifica Inc. dba IT&E**, a wireless provider headquartered at 122 Harmon Industrial Park Rd, Tamuning, Guam 96913.

ATTACHMENT B

Particular Things to be seized

I. Information to be disclosed by PTI Pacifica Inc. dba IT&E

To the extent that the information described in Attachment A is within the possession, custody, or control of **PTI Pacifica Inc. dba IT&E**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **PTI Pacifica Inc. dba IT&E** or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **PTI Pacifica Inc. dba IT&E** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages **December 1, 2019 to Present** stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from **December 1, 2019 to Present**;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message from **December 2019 to Present**;
- e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account,

Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from **December 1, 2019 to Present;**

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from **December 1, 2019 to Present;**

h. Incoming and outgoing telephone numbers, from **December 1, 2019 to Present;**

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between **PTI Pacifica Inc. dba IT&E** and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) and 846 involving Aaron Matthew Pangelinan since December 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The acquisition and sale of illegal drugs, including methamphetamine, to include discussions regarding the receiving and disposition of the proceeds of such sales.

b. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

c. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

d. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;

e. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).

f. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the sale of methamphetamine, including records that help reveal their whereabouts.